REMARKS

The above amendment and these remarks are responsive to the Office Action of Examiner Kyung H. Shin of 26 Aug 2005.

Claims 1-10, 13, and 15 are in the case, none as yet allowed.

35 U.S.C. 103

Claims 1-15 have been rejected under 35 U.S.C. 103(a) over Salas et al (Salas, U.S. Patent 6,233,600) in view of Maurille (U.S. Patent 6,484,196) and further in view of Cutler et al. (U.S. Patent 5,129,083). Applicants note that claims 11, 12, and 14 were previously canceled, and are no longer being asserted in the case.

Applicants have amended claims 1, 3, 8, 9, 10, 13 and 15.

In addition, Applicants traverse, and argue that the Examiner has not established a prima facie case of obviousness, which requires that the Examiner provides

1.   one or more references
2.   that were available to the inventor and
3.   that teach
4.   a suggestion to combine or modify the references,
5.   the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of ordinary skill in the art.

LOT919990047US1   14   S/N 09/473,098

The fourth element of the prima facie case, the suggestion to combine, must come from the prior art. It is insufficient to establish obviousness that the separate elements of the invention existed in the prior art, absent some teaching or suggestion, in the prior art, to combine the elements. That a claimed invention may employ known principles does not itself establish that the invention would have been obvious, particularly where those principles are employed to deal with different problems. The Examiner must consider the claim as a whole, and not piece together the claimed invention using the claims as a guide. The Federal Circuit has stated: "[o]ne cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention. [See In re Fritch, 23 USPQ 2d 1780, 1784 (Fed. Cir. 1992)].

In this case, applicants assert that the Examiner has not established a prima facie case of obviousness, but has rather used applicants' own disclosure as a road map for assembling teachings from the Salas, Maurille, and Cutler references. Applicants further contend that these teachings are not from a common domain such that teachings may be combined as the Examiner asserts. Typical of the Examiner's rationale for combining these references is the following:

> "It would have been obvious to one of ordinary skill in the art... to modify Salas to operate a collaborative workspace for message communications between members as taught by Maurille, and to modify Salas to enable utilization of standard object oriented techniques for collaborative space processing such as pointers to objects containing access control lists (ACLs) and controlling access to objects as taught by

LOT919990047US1   15   S/N 09/473,098

Cutler.... to employ Maurille in order to optimize message processing and display capabilities for a networked collaborative communications environment (see Maurille col. 6, lines 13-16...), and to employ Cutler in order to efficiently enhance security by providing limited visibility of computer resources and pretecting data integrity (see Cutler, col. 1, lines 47-53...).

The above statement falls short of demonstrating that Salas, Maurille and Cutler teach applicants claims, either as previously presented or as currently amended. That is, various teachings are drawn from these references in an apparent attempt to show all of the elements of applicants claims, yet they fail to do so at the level of specificity set forth in applicants claims.

Further, these references are in different fields, or domains. Specifically, Cutler refers to objects within an operating system domain, which is not the same domain as collaboration space. Maurille contains no reference to rooms in collaboration space. The generic use of access control on objects in an operating system taught by Cutler does not map, to those of ordinary skill in the art, to the specific claimed configuration of access controls on rooms and subrooms which are places within collaboration space having access control lists in each room and readers fields on forward pointers between rooms. Salas refers to an E-room, which is not the same as applicants collaboration space. The Salas E-room is a database with tables on a server, but not a plurality of E-rooms. Applicants collaboration space does not refer merely to a database on a server, but rather to a construct that has a plurality of rooms linked in such a way that a quick place includes a

LOT919990047US1   16   S/N 09/473,098

plurality of quick places double linked with access control
on each parent place, each child place, and each forward
pointer linking these places.

Applicants collaboration space comprises a root place
including a plurality of additional places (subrooms) linked
by the double linked (forward and reverse pointers)
construct set forth in the claims, with access control on
the root place, each subroom, and on the forward pointers
which, in combination, support increased, decreased, and
maintained (the same) access to the subroom as that allowed
on a parent room, and that access at any level of authority
to a subroom is enabled only for those authorized to access
the root room, together with a third access control provided
on forward pointers to control whether the link to a child
room will be enabled in its parent room for a specific user.

The Cutler reference is newly cited, and characterized
by the Examiner as teaching "...the usage of object oriented
technology utilizing access control list techniques for
collaborative space management". Applicants agree that
Cutler teaches access control on objects in an operating
system domain, but traverse the suggestion that Cutler
teaches such for collaborative space management. The
Examiner refers to the following from Cutler:

> "In addition to visibility control, access to each
> object is controlled through an access control list
> which specifies the processes authorized to access the
> object, and the types of access that are allowed."
> [Cutler, Col. 2, lines 27-30.]

> "Each object 822 has access control information

LOT919990047US1   17   S/N 09/473,098

that describes the access rights needed by a user to gain access to a resource. The object header 820 contains the access control information." [Cutler, Col 22, lines 65-67.]

"Any process, including the top level process, can cause the creation of additional processes, called subprocesses or child processes. Any process which creates another process is referred to as a parent process." [Cutler, Col. 5, lines 21-25.]

There is no teaching in Cutler, nor in Cutler in combination with Salas and Maurille, that a second access control list is provided for a subroom (each room and subroom is a separate quick place in a collaboration domain) in a hierarchy of rooms (or quick places) so as to enable increased, decreased, and maintained (the same) access to the subroom as that allowed by the access control list on the parent room, and that access at any level of authority to a subroom is enabled only for those authorized to access the root room, together with a third access control (readers field) on the forward pointer to control whether the link to a child room will be enabled in its parent room for a specific user.

In Applicants' invention, an access control list for the place in collaboration space is used for management of security of rooms within that space. That is, access to rooms within a place is limited to only those individuals listed in the access control list for the place. Thus, Applicants' invention provides a restrictive control over who may become a member of the various rooms within a place (that is, to whom managers can give access to rooms within the place.) This list of people are in the place main or

LOT919990047US1   18   S/N 09/473,098

root room of the hierarchy of rooms. A manager or author
can only add to the access control list of a room or subroom
individuals who are listed in the access control list of the
root room of the hierarchy. This structure is brought out
in the following references from the specification.

"Referring again to Figure 6, eight QuickPlace
extensions 160 are enhancements made to the Domino web
server 132 in order to support a QuickPlace
application. These extensions 160 are enabled only for
QuickPlace URLS; that is, they are enabled for URLs
that are targeted against a particular QuickPlace.
These extensions are: (1) shared design elements, (2)
database linkage, (3) commands, (4) publish and draft
model, (5) security and authentication, (6) forms and
fields, (7) decoration model), and (8) graphics
server." [Page 56, line 13 to page 57, line 1. Emphasis
added.]

"(2) Database linkage enables the grouping of a
number of databases in a hierarchical way. A place is
a collection of databases, and these need to be
represented in a parent child relationship. Data notes
represent the hierarchy to the database. There is a
data note in the parent database, and there is a data
note in the child database. The use of data notes for
these QuickPlace extensions as a way of representing
their functionality has the benefit that there are many
ways of manipulating them, whether it's with Java or
forms or the Notes designer. [Specification, page 57,
lines 12-21.]

"(5) The security and authentication QuickPlace
extension is consistent with the QuickPlace model,
which provides three levels of security or roles:
reader, author, and manager. There exists a member

LOT919990047US1   19   S/N 09/473,098

directory for each place. What this means is that each place has its own set of members that visit it. The Domino server is modified to perform local authentication against that directory, making places very portable, self-contained. And they don't collide with other members in other places. A user, having control of his own place member directory, set his own security for access to that directory. [Page 59, line 15 to page 60, line 1. Emphasis added.]

"...a collaborative environment to be set up without administrative support, that is by members of the team itself, using a familiar and easy to use browser user interface. Members of the team, acting with manager or author authority, and using such a browser interface without involving administrative or application development support, need to be able to set up a folder or room for each project element..." [Specification, page 5, lines 7-15. Emphasis added.]

"A room is created from a default room type template, PageLibrary.ntf, which provides indexing infrastructure for maintaining the pages in a room, and also security and authentication features so that access to a room can be limited to a subset of team members." [Specification, page 55, line 16 ff. Emphasis added.]

Applicants contend that nowhere does Salas, Maurille, or Cutler teach that membership in an access control list control on a specific subroom in collaboration space is limited to members included in the access control list for the collaboration space. Thus, the reference to Col. 13, lines 31-34 of Salas states:

"...each object may be provided with a field or fields

LOT919990047US1   20   S/N 09/473,098

which identify users that may open, view, and edit the
object."

"Users" is not limited, apparently, to "members", as the
latter may be identified for the place as distinguished from
objects within the place. As noted above, Cutler does not
provide this missing element from Salas.

Applicants invention provides a double linked list for
linking rooms together in collaboration space, with access
control list control on rooms and access control list
control on forward pointers, or child pointers, to child
rooms.

This structure is illustrated in Figures 10 and 11 of
applicants' specification, which are described as follows:

> Referring to Figure 10, QuickPlace rooms 201-204
> and 210 are connected by forward and backward pointers
> 205-209 and 211, and these enable the security of each
> room to be independently managed. Each room has its
> own security; that is, the identity of each user
> allowed to enter the room and that users security
> level: the three levels being reader, author, manager.
> This is held in an access control list which is a part
> of each room. While an individual, say Steve, has
> reader access (R) to the library 204, he can have
> author (A) access to a subroom 211. This enables a
> subroom 211 to have increased/ maintained, or decreased
> access authority for a particular individual with
> respect to its parent room 204. Only individuals with
> access to a parent 204 can access a subroom 210, but
> that subroom 210 can have changed access for the
> subroom 210 for these individuals. Previously,

LOT919990047US1   21   S/N 09/473,098

security could not be increased in subrooms 210 with respect to a parent room 204.

A database access control list (ACL) specifies who can or cannot access the database. For users who can access a database, access levels and roles determine the specific actions they can perform -- for example, creating or deleting documents. Document access fields (Readers and Authors fields), in conjunction with the database ACL, control who can read or modify specific documents. Thus, to limit access to specific documents created from a form, a readers field is included. A readers field explicitly lists the users who can read documents created from the form. If a form has an access list, names from the readers field are added to the form access list. Otherwise, the readers field controls access to documents created from the form. Entries in a readers field cannot give a user more access than what is specified in the database access control list (ACL); they can only further restrict access. An authors field works in conjunction with author access in the database ACL. Listing users in an authors field expands access rights by allowing listed users to edit documents they create. Entries in an authors field cannot override the database access control list; they can only refine it. Authors fields affect only users who have author access to the database.

Referring to Figure 11, _forward pointers 205, 209 are secure_. Security, in this context provides that forward pointer 205 to project A 203 carries the same security as that of project A 203, and anyone viewing main room 201 who is not entitled to access project A 203 will not see room 203 listed in parent room. QuickPlace does not show a user things or objects to which the user does not have access. In past, such

LOT919990047US1   22   S/N 09/473,098

objects were shown, but were greyed out or otherwise managed so that user access was inhibited. Forward pointers, therefore, include room name field 212, address to database name field 213, and readers field 214, which includes a table of user identifiers 215 for each user permitted to access the room, with corresponding access authority 216 for each such user, which may be manager, author, or reader. [Applicants' specification, pages 48-50.]

None of the references cited, taken individually or in any combination, teaches this structure of a double linked list for linking rooms together in rooms (places) in collaboration space with ACL security on each room (place in collaboration space) and ACL security (readers fields) on forward pointers in the double linked list.

The Examiner refers to Salas col. 3, lines 49-51 and col. 13, lines 32-34 as teaching a "readers field for providing access control list control on said forward pointer." [Office Action, page 3.] Applicants traverse. This is what Salas teaches:

"The server database 20 stores various tables which contain information about eRooms, members, access controls, and other data objects." [Salas, Col. 3, lines 49-51.]

"For example, each object may be provided with a field or fields which identify users that may open, view, and edit the object." [Salas, Col 13, lines 32-34.]

Applicants assert that there is no teaching here of an access control list, or readers field, on a specific forward

LOT919990047US1   23   S/N 09/473,098

pointer from a parent room to a child room, which ACL or
readers field is distinct from the ACL for the parent room.
Applicants structure of access control elements provides a
readers field as part of the pointer which is distinct from
the ACL on either the parent or the child room, and is an
ACL control on the pointer itself used to specify whether a
pointer to a child room (place) is enabled in its parent
room (place). Cutler teaches access control on objects
generically, but does not teach using such in collaboration
space, as previously stated. Thus, neither Salas nor
Maurille nor Cutler disclose or teach such a structure.

The Examiner refers to Maurille as teaching forward
pointers identifying a child room, but is silent as to the
existence of an ACL control on that pointer [Maurille, Col.
6, lines 44-57]. However, applicants note, Maurille has no
teaching of "room" entities, and only refers to a data
schema including users, not rooms in collaboration space.

Consequently, the combination of Cutler, Salas and
Maurille does not teach, applicants argue, ACL control
specific to forward pointers in the hierarchical structure
of rooms in collaboration space together with ACL control on
the parent and child rooms within that space.

That Salas does not teach a double linked list with ACL
security on forward pointers in addition to ACL security on
the rooms is apparent from examination of Salas Figure 1,
which does not show forward and reverse pointers between
rooms. In Salas, there is no teaching of forward and
reverse pointers linking rooms with ACL security on those
forward pointers, as distinguished from and in addition to

LOT919990047US1   24   S/N 09/473,098

security on the rooms. While Maurille may disclose forward and reverse pointers, none of Cutler, Maurille or Salas teach ACL security on the forward pointers. Cutler's generic teaching of ACL on objects in an operating system domain does not teach the specific configuration of ACL controls on rooms and pointers within a collaboration space domain.

Maurille is cited by the Examiner as teaching databases and pointers linking them, and Applicants agree that such is taught. Cutler is cited by the Examiner as teaching access control lists, and Applicants agree that such is taught. Applicants do not claim they invented forward and reverse pointers between objects in a hierarchy, nor are they claiming they invented access control lists. Rather, Applicants invented a hierarchy of rooms to create a collaboration space with a specific protocol of access control lists, including ACL lists on rooms and additional ACL control specifically on forward pointers used for management of security of rooms within that collaboration space. Neither Maurille, Cutler, nor Salas, taken separately or in combination, teach that protocol.

SUMMARY AND CONCLUSION

Applicants urge that the case be passed to issue with claims 1-10, 13, and 15.

The Application is believed to be in condition for allowance and such action by the Examiner is urged. Should differences remain, however, which do not place one/more of

LOT919990047US1   25   S/N 09/473,098

the remaining claims in condition for allowance, the Examiner is requested to phone the undersigned at the number provided below for the purpose of providing constructive assistance and suggestions in accordance with M.P.E.P. Sections 707.02(j) and 707.03 in order that allowable claims can be presented, thereby placing the Application in condition for allowance without further proceedings being necessary.

Sincerely,

J. Estrada, et al.

By

Shelley M Beckstrand
Reg. No. 24,886

Date: 20 Oct 2005

Shelley M Beckstrand, P.C.
Patent Attorney
61 Glenmont Road
Woodlawn, VA 24381-1341

Phone: 276 238-1972

LOT919990047US1   26   S/N 09/473,098